الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش

Cyber War in the Digital Age: Post-Clausewitz Wars



زينب شنوف

المدرسة الوطنية العليا للعلوم السياسية، الجزائر، zeinebchpolitics@gmail.com

تاريخ الإرسال:2020/02/21 **تاريخ القبول:** 2020/03/10 **تاريخ النشر:** 2020/07/01

ملخص:

*تفترض هذه الدراسة أن الحرب السيبرانية هي نمط جديد من الحروب في العصر الرقمي، تعكس التحول عن المفهمة الكلاسيكية للحرب عند **(كلاوزفيتش)**. بالاعتماد على المنهج الوصفي-التحليلي، يهدف المقال إلى تقديم تحليل معمق للحرب السيبرانية، والنقاش الأكاديمي والسياسي حول دورها في البيئة الاستراتيجية العسكرية، وكيف ساهمت خصائصها بجميع عناصرها الثورية في تغير الحرب في العصر الرقمي، لتشكل تهديدا فعليا على أمن الدول، ما طرح إشكالية مضمونها: هل الاستراتيجيات الكلاسيكية كافية لمواجهة الحرب السيبرانية؟ خلص هذا المقال الى نتيجة: تعبر الحرب السيبرانية عن طابع حربي جديد، أحدث تطورات ثورية في شن الحروب، وسياسات الدفاع، ونموذج (كلاوزفيتش) للحرب يجب استبداله بأعمال نظرية أكثر ملاءمة للعصر الرقمي.*

الكلمات المفتاحية: *الحرب السيبرانية؛ الفضاء السيبراني؛ العصر الرقمي؛ الاستراتيجية السيبرانية.*

Abstract:

This study argues that cyberwar is a new kind of warfare in the digital age; which alters the classical Clausewitzian understanding of war, Based on descriptive-analytical methods, The article aims to offer an in-depth analysis of cyberwarfare, and outlining the theoretical and political debate around its role in the strategic military environment, It then describes how the characteristics of cyberwar effect on the transformation of war, to become the real threat to the national security, This poses a problematic: are classical strategies effective against cyberwar? In summary; the paper argues that cyberwar is a new form of war; which entails a change in the warfare, and the Defense Policies, and the Clausewitzian model of war must be replaced by a new theoretical work adapted to the digital age.

Keywords: *Cyber War; Cyberspace; Digital Age; Cyber Strategy.*

* المؤلف المرسل: زينب شنوف، zeinebchpolitics@gmail.com

مقدمة:

شكلت الثورة الرقمية والمعلوماتية قفزة تكنولوجية، خلقت مجتمع رقمي تأثيراته حسب (**ألفين توفلر**)، و(**هايدي توفلر**) من المقرر أن تعيد تشكيل الأساس الاقتصادي للمجتمع الحديث، وبالتالي تحويل التجارة والسياسة، والعلاقات الاجتماعية، وحتى النزاعات. كما أشارت (ماري كلدور) Marry Kaldor في كتابهاNew And Old War إلى أنّ توظيف تكنولوجيا المعلومات في القطاع العسكري أثار النقاش بين الاستراتيجيين الأمريكيين حول ما يعرف باسم الثورة في الشؤون العسكرية، أو تحويل سياسات الدفاع (Kaldor, 2012, P07)، وأنّ مخرجات هذا التوظيف تُشكل المحرك الأساسي للخصوصيات الجديدة للحرب ما أدى إلى تغير البيئة العملياتية للحروب، وظهور فضاءات جديدة آخرها الفضاء السيبراني.

ولقد أدى تزايد عدد الهجمات السيبرانية التي تشنها بعض الدول، والفاعلين من غير الدول أشهرها **فيروس ستاكسنت Stuxnet** الذي عطل البنية التحتية لتخصيب النووي الإيراني في عام 2010. وتسبب في أضرار مادية عبر الحدود الدولية، إلى الإعلان عن شكل جديد من الحروب في العصر الرقمي، الذي يهدد حتى أقوى القوى العسكرية. كما أنّها منحت الجهات الفاعلة العسكرية الأضعف مزايا غير متماثلة. وتُجسد الحرب السيبرانية مثالا واضحًا للحرب عن بُعد حيث يمكن للدول الدخول في عمليات هجومية ضد دول أخرى، وتحقيق الأهداف الاستراتيجية، دون الحاجة إلى الاشتباك معها، وغالبًا ما يكون ذلك في سرية تامة، هذه الخصائص جعلت الحرب السيبرانية، تتحدى الأفكار الكلاسيكية لـ (**كلاوزوفيتش**) حول طبيعة الحرب، خاصة مركزية العنف، واشتباك الجيوش وسط الضباب، ودعت إلى ضرورة مراجعة سياسات دفاع الدول، وهذا ما تضمنته العقيدة العسكرية للدول الخمس الدائمة العضوية في مجلس الأمن التابع للأمم المتحدة، جميع هذه الدول تتفق على أن الأحداث السيبرانية تزداد أهمية، وأنّ الاستراتيجيات العسكرية الكلاسيكية غير مستعدة للنزاع في العالم الرقمي أو السيبراني.

حسب ما تم ذكره يهدف هذا المقال، وبالاعتماد على المنهج الوصفي التحليلي إلى الإجابة عن الإشكالية التالية: ماهي المحددات الاستراتيجية التي تثبت أنّ الحرب السيبرانية هي طابع حربي جديد يجسد التحول عن المفهمة الكلاسيكية للحرب عند (**كلاوزفيتش**) ويتطلب استراتيجيات جديدة لمواجهتها؟

للإجابة على هذه الإشكالية تقترح الدراسة الفرضية التالية: الحرب السيبرانية تعبر على نوع جديد من الحروب ترتكز على قاعدة المعرفة في القتال، والتأثير الرقمي لتحقيق الأهداف الاستراتيجية توحي بالتحول عن المفهمة الكلاسيكية للحرب عند (**كلاوزفيتش**) التي ترتكز على المعركة. كما أنها تفرض على الدول تطوير عقيدة وسياسات دفاعية جديدة تكيفاً مع هذا التحول.

وسيتم معالجة الإشكالية من خلال تناول العناصر التالية:

- ✓ الحرب السيبرانية المفهوم وجدلية التوظيف العسكري
- ✓ خصائص الحرب السيبرانية ومحددات تغير الحرب في العصر الرقمي
- ✓ الحرب السيبرانية وتطور الاستراتيجية العسكرية للدول

1.الحرب السيبرانية المفهوم وجدلية التوظيف العسكري

تحديد ماهية الحرب السيبرانية بدقة خلق مشاكل عملية، وجدلا بين المفكرين الاستراتيجيين، فبعضهم يعتبرها مجرد أداة استراتيجية غير مستقلة، لا ترقى إلى صفة الحرب، في حين يجادل صنف آخر أنها تمثل طابع حربي جديد. يعبر عن التغير في المفهمة الكلاسيكية للحرب عند **(كلاوز فيتش)**، بناء على ذلك جاء هذا المحور ليحدد هذا المفهوم، حتى يتم توظيفه بما يتفق وطرحنا لهذا الموضوع.

أ.مفهوم الحرب السيبرانية «cyberwarfare»: عرفت **وزارة الدفاع الأمريكية الحرب السيبرانية بأنها** "توظيف القدرات السيبرانية حيث يكون الغرض الأساسي هو: تحقيق الأهداف أو الآثار العسكرية في الفضاء السيبراني أو من خلاله." يضيف تقرير خدمة أبحاث الكونغرس لعام 2001 "يمكن استخدام مصطلح الحرب السيبرانية لوصف الجوانب المختلفة للدفاع، ومهاجمة شبكات المعلومات، والحواسيب في الفضاء السيبراني، فضلاً عن حرمان الخصم من القدرة على فعل الشيء نفسه." (Schreier, 2015,P16).

ووفقًا للقرار الصادر عن مجلس الأمن الدولي مؤخرًا، "الحرب السيبرانية هي استخدام أجهزة الحاسوب، أو الوسائل الرقمية من قبل حكومة، أو بمعرفة أو موافقة صريحة من تلك الحكومة ضد دولة أخرى، أو ملكية خاصة داخل دولة أخرى بما في ذلك: الوصول المتعمد أو اعتراض البيانات، أو تدمير البنية التحتية الرقمية. وإنتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي. (Schreier, 2015, P16)..

وتعني أيضا "نشاط متماثل أو غير متماثل، دفاعي أو هجومي على الشبكة الرقمية، من قبل فواعل دولية أو غير دولية، يهدف إلى إلحاق الضرر بالبنية التحتية الحيوية الوطنية، والأنظمة العسكرية." (Schreier, 2015, P10) والتأثير على إرادة وقدرات صنع القرار في القيادة السياسية للعدو، والقوات المسلحة، أو مواقف السكان المدنيين في مسرح العمليات على مستوى نظم المعلومات".(Cavelty 2010, P1).

والحرب السيبرانية هي جزء فرعي من حرب المعلومات التي تنطوي على استخدام ساحة المعارك، وإدارة تكنولوجيا المعلومات، والاتصالات في السعي لتحقيق ميزة تنافسية على الخصم." (http://bit.ly/2OH4UkG)، يُعرّفها رؤساء الأركان المشتركة بأنها التوظيف المتكامل للحرب السيبرانية، وأنشطة شبكات الحاسوب، والحرب النفسية، والخداع العسكري، وأمن العمليات، بالتنسيق مع قدرات داعمة، وما يتصل بها مع إمكانية التأثير أو الإخلال على قدرات العدو". الفكرة الرئيسية لفهم حرب المعلومات هي أن أساسها المركزي هو استخدام المعلومات أو البيانات كسلاح (Peifer1997, Pp32-33)، ففي أواخر السبعينيات تم الاعتراف بدورها الحاسم كعنصر من عناصر القوة، **جعل القوات المسلحة تنظر إليها باعتبارها كفاءة عسكرية أساسية، وأنّ المعلومات هي سلاح، وهدف في الحرب**، ويعتقدون أن تفوق المعلومات والمعرفة يمكن أن يحقق النصر في الحروب (Dragan 2017, P1045).

كما تختلف **الحرب السيبرانية عن الحرب الالكترونية(Netwar)**، كون الحرب الإلكترونية تعني النزاعات السيكولوجية على المستوى المجتمعي التي نشبت جزئياً من خلال أساليب الاتصالات المختلفة، أما "الحرب السيبرانية" فهي التي نشبت على المستوى العسكري (والتي يركز عليها هذا المقال) كل من الحرب الالكترونية Netwar والسيبرانية Cyberwar يدوران حول مسائل المعلومات والاتصالات، إلا أن الحرب السيبرانية تدور على مستوى أعمق من أشكال الحرب حول معرفة إستراتيجيات تأمين مجتمع أو جيش، يساعد

هذا التمييز في تحديد مدى السبل التي قد تغير بها الثورة المعلوماتية والرقمية طابع النزاع إلى جانب الحرب، وكذلك سياق الحرب وسلوكها. (http://bit.ly/2BXXEv9).

ضمن مفهوم الحرب السيبرانية، يجب التمييز بين شكلين من عمليات شبكة الحاسوب **الهجوم السيبرياني Cyber Attack** الذي يُطلق على الشلل المتعمد، أو تدمير قدرات شبكة معلومات العدو (Cavelty, 2010, P2)- مثل سرقة المعلومات من أجهزة التخزين، الهجوم على العمليات التي تقوم بجمع، وتحليل، ونشر المعلومات باستخدام أي وسيط أو نموذج، والهجوم على نظم المعلومات والاتصالات (Peifer, 1997, Pp32-33)، والدفاع السيبراني **Cyber Defense** وهو عبارة عن آلية للدفاع عبر شبكة المعلومات، والتي تركز على منع، وكشف، وتوفير الاستجابات في الوقت المناسب للهجمات أو التهديدات، بحيث لا يتم العبث بالبنية التحتية أو المعلومات. (Galinec, and others, 2017, p274).

وحتى يكتمل تحديد معنى مفهوم الحرب السيبرانية لابد من التعرف على مكوناته الأساسية:

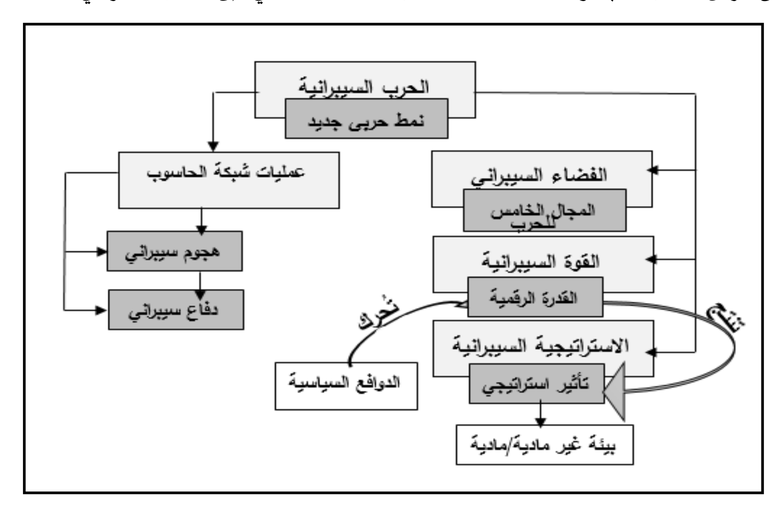
الفضاء السيبراني Cyberspace: الفضاء السيبراني هو المجال الخامسة للحرب، يُشير إلى البيئة التي أنشأها التقاء الشبكات التعاونية لأجهزة الحاسوب، وأنظمة تكنولوجيا المعلومات، والبنى التحتية للاتصالات، يشار الیها باسم شبكة الويب العالمية«The World Wide Web (Wingfield, 2000, P1). **تُعرفه وزارة الدفاع الأمريكية**: "على أنّه مجال يتميز باستخدام أجهزة الحاسوب، والأجهزة الإلكترونية الأخرى لتخزين، وتعديل وتبادل البيانات عبر الأنظمة الشبكية، والبنى التحتية المادية المرتبطة بها، وهو مجال عملياتي له طابع مميز، وفريد **يختلف نوعياً عن مجال البحر، والهواء، والفضاء، ومع ذلك هناك تداخل وظيفي بينهم، كما أنه الأكثر أهمية**، فهو المجال الوحيد الذي تلتقي فيه جميع أدوات القوة الوطنية، وتُمارس في وقت واحد. (http://bit.ly/33d3Ryu)

القوة السيبرانية Cyberpowere: تمثل القدرة على الحصول على النتائج المفضلة، من خلال استخدام موارد المعلومات المترابطة إلكترونيًا في المجال السيبراني، وهي مجموع التأثيرات الاستراتيجية الناتجة عن العمليات السيبرانية في الفضاء السيبراني، وفي مجالات أخرى خارج الفضاء السيبراني، وفي تعريف آخر القوة السيبرانية هي "القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير الاستراتيجية على الأحداث في البيئات العملياتية الأخرى، وعبر أدوات القوة المختلفة." (Schreier, 2015 ; P18)

الاستراتيجية السيبرانية cyberstrategy: هي تطوير وتوظيف القدرات اللازمة للعمل في الفضاء السيبراني، متكاملة مع المجالات العملياتية الأخرى لتحقيق أو دعم تحقيق الأهداف عبر عناصر القوة الوطنية. تعتمد الاستراتيجية السيبرانية على مزيج منظم من الغايات، والوسائل، والطرق (كيفية استخدام الوسائل). لتحقيق أهداف الأمن العسكري والسياسي، والاقتصادي، والدبلوماسي، والوطني الأوسع، من خلال الاعتماد على القدرات السيبرانية، وتوفير الموارد، والتكاليف الواجب اتخاذها لمواجهة المخاطر. وعليه تتمثل المساهمة الرئيسية للاستراتيجية الوطنية للفضاء السيبرانية في توضيح صريح لكيفية تحقيق جميع الاستراتيجيات الأخرى، ولا سيما استراتيجية الأمن القومي (Schreier, 2015, P18).

التعريف الإجرائي للحرب السيبرانية: (أنظر الشكل:1) الحرب السيبرانية هي حرب نشأة في الفضاء السيبراني، **تستخدم التأثير الرقمي الذي تحركه دوافع سياسية**، لإجبار الخصم على تنفيذ إرادة الطرف

المهاجم، يمكن أن تعرف أيضا على أنها نزاع عسكري في الفضاء السيبراني، الذي يمثل مجالا جديد للحرب وبعدا إضافيا مكملا للحرب التقليدية، يستخدم تكنولوجيا المعلومات، لإلحاق الضرر بشبكات وأنظمة العدو، وكذلك خلق فرص للمناورة الهجومية، تأثيراته قد تتجاوز المجال السيبراني، إلى الحاق الضرر في مجالات أخرى.



شكل رقم1-*تعريف الحرب السيبراني*-

المصدر: من إعداد الباحثة

من العرض السابق يتضح أن الحرب السيبرانية لا تعتمد على الاشتباكات التقليدية العنيفة بين القوات العسكرية، مُتحدية بذلك فكرة **(كلاوزفيتش)** عن **مركزية العنف** في الحرب، هذا ما خلق جدلا نظري بين المفكرين حول ما إذا كانت الحرب السيبرانية تشكل فعلا نوعا جديدا من الحروب في العصر الرقمي، يمكن توظيفه في القطاع العسكري بما يحقق الفعالية الاستراتيجية للدول.

<u>ب. الجدل النظري حول الحرب السيبرانية والتوظيف في القطاع العسكري</u>: حتى نثبت أنّ الحرب السيبرانية تمثل فعلا ونمطا جديد من الحروب في العصر الرقمي، يجب تحديد السياق الذي تستخدم فيه، غياب هذه الخطوة كما أشار **(توماس ريد)Rid Thomas**، غالبًا ما يسمح بسوء تطبيق ما يعنيه المرء بالحرب في المقام الأول. وهذا ما ذهب إليه **(كلاوزفيتش)** منذ وقت طويل بقوله: "المعرفة بطبيعة الحرب ضرورية لإدارة التفاعل السياسي". (Brandon and Manes, 2015;P15).

نزع الطابع الحربي عن الحرب السيبرانية: يجب أن يحمل القتال السيبراني بعض الصفات المستقلة، حتى يُشكل نمطا جديد للحرب. رغم ذلك يرى **(كولين جراي)** "colin gray": أنّه "حتى لو كان للقتال السيبراني بعض الصفات المستقلة، فلا يزال يجب أن يحدث في السياق السياسي، والاستراتيجي للحرب" (Mahnken , 2011, P58).بناءا على ذلك لا يمكن مناقشة مسألة الحرب السيبرانية دون فهم ما نعنيه بالحرب من الناحية الإمبريقية، وكيف ترتبط بالخطاب السياسي.

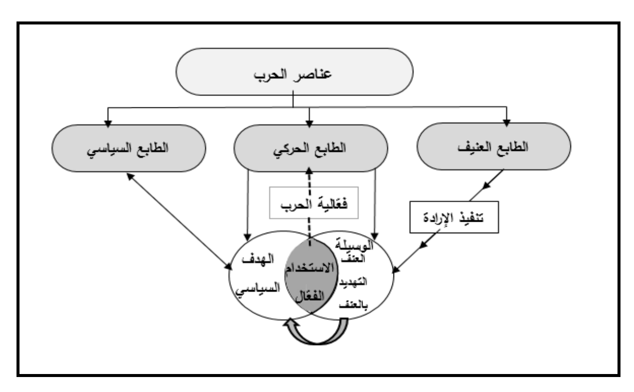
شرح (**كلاوزوفيتش**) **Clausewit** و(**هيدلي بول**). **Hedley Bul** **جوهر** الحرب حيث يخبرنا البروسي أن "الحرب هي عمل من أعمال العنف لإجبار عدونا على القيام بإرادتنا، وأنها ليست سوى مبارزة على نطاق أوسع"، يتفق معه (**هدلي بول**) ويكتب "الحرب هي عنف منظم تمارسه الوحدات السياسية ضد بعضها البعض." (Colin, 2006, p186)

ويضع (**كلاوزفيتش**) **ثلاثة معايير رئيسية** (شكل:2) **لأي عمل عدواني أو دفاعي يطمح إلى أن يكون عملاً حربياً قائماً بذاته،** أو قد يتم تفسيره على هذا النحو، ما يعني حتى يتم وصف الهجمات السيبرانية على أنها حرب لا بد من أن تجتمع هذه العناصر الثلاث. (Rid, 2013, P01).

العنصر الأول هو الطابع العنيف للحرب: "، حقيقة أن الحرب تنطوي على القوة تفصلها عن أنواع أخرى من المنافسة السياسية، والاقتصادية، والعسكرية. تتضمن الحرب تورطها في العنف وسفك الدماء والقتل..(Mahnken , 2011, P58) وكتب (**كلوزفيتش**) في الصفحة الأولى من كتابه **On War**: "**إذا لم يكن الفعل عنيفًا، في هذا السياق فهو ليس عملا حربيا**، وليس هجومًا مسلحًا، واستخدام الكلمة سوف يكتسب بُعدًا مجازيًا، لأن النشاط الفعلي للحرب، أو الهجوم المسلح يكون دائما قاتلا، على الأقل من جانب أحد الأطراف المشاركة ضد الطرف الآخر".(Rid, 2013, P01)

العنصر الثاني الذي ركز عليه **(كلاوزوفيتش) هو الطابع الحركي للحرب**: دور الحرب يكون دائما فعّالا، ولكي يكون فعالًا يجب أن يكون هناك **وسيلة وأهداف**: العنف الجسدي أو التهديد باستخدام القوة هو الوسيلة، وإجبار العدو على قبول إرادة الجاني هو الهدف. مثل هذا التعريف "ضروري من الناحية النظرية"، استخدام الخصوم للعنف بطريقة فعّالة في الحرب يشير إلى الاستخدام الفعال للوسائل على المستويات التكتيكية والعملياتية، والاستراتيجية والسياسية.

وهذا يؤدي إلى **الميزة الثالثة** والأكثر مركزية للحرب **طبيعتها السياسية:** يكون الهدف الأكبر للحرب دائمًا سياسيًا، إنه يتجاوز استخدام القوة، ولقد لخص (**كلوزفيتش**) ذلك بعبارة "الحرب هي مجرد استمرار للسياسة بوسائل أخرى.(Rid, 2013, Pp01-02)، **فإذا لم يتم تطبيق القوة لأغراض سياسية، فهي ليست حربًا**. (Colin, 2006, p186)

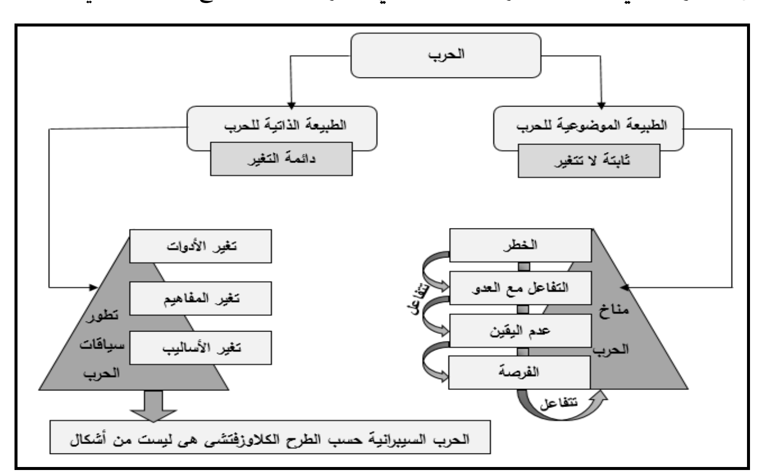


الشكل: رقم 2.1- *عناصر الحرب عند كلاوزفيتش*-

المصدر: من إعداد الباحثة

أما في العصر الحديث يعرف **(توماس ريد)** الحرب قائلا: هي نزاع عسكري ينشب بين كيانات وطنية، تكون الدولة أحد أطرافها، مما يؤدي إلى مقتل على الأقل 1000 شخص من العسكريين. يجب أن تُذكر هذه النقطة المفتاحية، **حيث أشار البعض إلى أنه لا يوجد في الواقع شيء من هذا القبيل في الحرب السيبرانية بحيث لا يكون هناك أي قتلى في المعارك السيبرانية** (Brandon and Manes, 2015; P28).

ما يعني أنّ العناصر التي تحدث عنها **(كلاوزفيتش) لا تتوفر في الحرب السيبرانية**، وهي كما يقول **(دان كافليتي) Dunn-Cavelty:** "التهديد السيبراني مبالغ فيه، فهو حتى الآن **مجرد أداة** شعبية للسياسيين، وصانعي السياسات، ومقاولي الدفاع في الخطاب المعاصر. (Brandon and Manes, 2015;P28). وهي لا تعبر عن نمط جديد للحرب، لأنّ الحرب حسب **(كولن غراي)** "هي سلوك مميز، **ولا يمكن أن تغير طبيعتها الموضوعية**، التي تبقى ثابتة، بغض النظر عن تطور الأسلحة، وتغير المحاربون، أو اختلاف وتغير القضايا. **وإذا غيرت الحرب طبيعتها، فإنها تصبح شيئا آخر غير الحرب**، على سبيل المثال "**مناخ الحرب**" "The climate of war" **لا يتغير مهما اختلفت خاصية القتال**، حيث يشتمل "المناخ" في أي فترة زمنية على "الخطر ، والجهد، وعدم اليقين والفرصةc، على النقيض من ذلك، فإن **الطبيعة الذاتية للحرب عرضة للتغيير الدائم** (Colin, 2006, p186) **وهي تعبر عن التحول الذي أحدثته الحرب السيبرانية في الحرب** حسب الطرح الكلاوزفيتشي.



شكل رقم: 3.1 –نزع الطابع الحرب عن الحرب السيبرانية-

المصدر: من إعداد الباحثة

على ضوء التعاريف السابقة، وبالاستناد إلى تصنيف **(كلاوزفيتش)** لطبيعة الحرب، إلى **طبيعة موضوعية تمثل جوهر الحرب لا تتغير باختلاف الزمان والمكان، وطبيعة ذاتية تتغير باستمرار**، يوضح الشكل أن العمليات التي تحدث في الفضاء السيبراني هي شيء مختلف عن الحرب التقليدية من حيث الجوهر، وأنها لا تحقق أحد أهم معايير **(كلاوزفيتش)** للحرب وهو العنف.

وهي حسب عدد من الأكاديميين مجرد تكتيك، وليس شكلاً من أشكال الحرب الكاملة، إنها أداة في الترسانة الدبلوماسية، والتفاعلات الدولية تماماً كغيرها من أشكال التهديد الموجودة لدى الدولة. (Westerburger, 2014, p37).

لكن يجادل فريق آخر من المفكرين بأن تعريف (**كلاوزفيتش**) للحرب وربطه بالعنف قديم، وأن ظهور الحرب السيبرانية يسمح بالتحول إلى تعريف (**صان تزو**) **Sun Tzu** للحرب: أي "**إخضاع العدو دون قتال**" على سبيل المثال: وصف (**فيليب ميلينجر**) **Phillip Meilinge** الهجوم السيبراني " بالغير الدموي، ولكنه يحتمل أن يكون طريقة جديدة للحرب".(Mahnken , 2011, P59)، بل وأكثر طموحًا من ذلك يدعي (**فرانسوا هيسبورغ**) **Francois Heisbourg** أن سلسلة التغيرات التكنولوجية، والسياسية، والاجتماعية، والاقتصادية "تُغير طبيعة الحرب"، وبالمثل يجادل (**أركيلا**) **Arquilla**، و(**رونفلت**) **Ronfeldt** أن الثورة الرقمية والمعلوماتية، ستأتي بالتحول في طبيعة الحرب، وهو ما يؤكده (**روبرت ليونارد**) **R.Leonhard Robert**: "إن عصر المعلومات يمثل أكبر **تغيير في طبيعة** الحرب". (Lonsdale, 2004, P16)

إذاً الحرب السيبرانية **هي نمط جديد للحرب**، ولقد أصبحت حقيقة واقعة، وهي حرب المستقبل القادمة، والفضاء السيبراني هو المجال الخامس للحرب، والمفاهيم الحديثة للحرب **تحتاج إلى إعادة النظر فيما يخص القتلى، والتطبيق المتعمد للقوة كشرط لوجود الحرب**، حسب (**جون ستون**) **John Stone** "الآثار العنيفة للحرب السيبرانية لا يجب أن تكون قاتلة لتقع تحت مفهوم الحرب". (Brandon and Manes, 2015;P28).

هناك بعض الحالات التي تُثْبِتُ أن الحرب السيبرانية وقعت فعلا من بينها: استخدام إسرائيل في سنة 2007 قدراتها السيبرانية في "**عملية البستان**"، ضد منشأة نووية سورية غير معلنة(http://bit.ly/2N3rq84)، كمثال آخر على الاستخدام العسكري للفضاء السيبرانية الهجمات السيبرانية في أوكرانيا: في مارس 2014، كما أعلنت الشركة العسكرية الروسية روستك "Rostec "عن الاستيلاء على طائرة أمريكية بدون طيار MQ-5B فوق شبه جزيرة القرم عن طريق التشويش الكهرومغناطيسي. (Saalbach, 2019, p47) **هذا الاستخدام "التقليدي" للقوة السيبرانية كسلاح عسكري ليس سوى أمثلة بسيطة، تدعو إلى ضرورة بناء نسق معرفي جديد للحرب يكون فيها الفضاء السيبراني مجالها الخامس**.

عند تطبيق المعيار المحوري الأهم لوصف أي نشاط حربي **"فعل عنيف"** " **Act Of Force**" على الحروب السيبرانية، من المرجح أن يكون الاستخدام الفعلي للقوة أكثر تعقيدًا من حيث الأسباب والنتائج التي تؤدي في النهاية إلى العنف والإصابات، Rid, 2013, P12). وكمؤثر بالمعنى الدقيق لكلمة "**العسكرية**"، استخدامها مثل أي سلاح تقليدي نعرفه من خلال إدخال أنظمة الأسلحة المعادية رقميًا، على سبيل المثال، يمكن أن يؤدي توجيه بنية إطلاق الصواريخ لتحويل التهديدات. (Westerburger, 2014, p37)، انهيار أنظمة النقل الجوي تاركةً مئات الطائرات بدون اتصال ما قد أن يخلف إصابات أو حتى قتلى، إمكانية عزل الوحدات العسكرية. **في مثل هذا السيناريوهات التدمير الذي تسببه الجريمة السيبرانية، دون شك يكون عملاً حربياً**، حتى لو لم تكن الوسائل **عنيفة وإنما العواقب فقط**. (Rid, 2013, P12).

إعطاء وزير الدفاع الأمريكي (**آشتون كارتر**) **Ashton Carte** في أوائل عام 2016، القيادة السيبرانية الأمريكية "أول مهمة لها في الحرب ضد (داعش)، وبالمثل تأكيد نائب وزير الدفاع البريطاني (**مايكل فالون**) **Michael Fallon** أن قدرات المملكة المتحدة السيبرانية قد تم نشرها في الحملة ضد داعش، هذان البيانان انضما إلى إعلان حلف الشمال الأطلسي "للاعتراف بالفضاء السيبراني كمجال خامس للعمليات الحربية"(http://bit.ly/2N3rq84).

مما سبق ذكره يتضح أن الحرب السيبرانية هي نمط جديد من الحروب، تسهل أشكال النزاع غير العنيف، لتتحدى بشكل مباشر تعريف **(كلاوزوفيتش)** لطبيعة الحرب، لكن في نفس الوقت على الرغم من أن هذه الأساليب ليست عنيفة، إلا أنها غالبًا ما تستخدم لتحقيق أهداف سياسية كان يمكن تحقيقها تاريخيًا من خلال العنف. حسب الطرح الكلاسيكي في حالة غياب العنف فإننا لن نتحدث عن الحرب بل عن السياسة الدولية، وهذا صحيح، إلا أنّ الرد على الهجمات السيبرانية قد يتعدى المجال السيبراني إلى الرد بالعنف المادي (القوة بالمفهوم التقليدي) في الواقع، ما يعني أنّ ظهور المجال السيبراني **لا يمنع العنف كوسيلة في الحرب بالمعنى الدقيق، وإنما يدعُو إلى توسيع تعريف العنف** إلى ما هو **أبعد من النزاع المادي**، كما جاء تعريفه عند **(كلاوزفيتش).** (http://bit.ly/33qNGNR)

2. خصائص الحرب السيبرانية ومحددات تغير الحرب في العصر الرقمي

ترجع أسباب تطور الحرب في العصر الرقمي عن المفهوم الكلاسيكي ل(كلاوزفيتش)، إلى التغير في طبيعة الفواعل والأهداف، ووسائل شن الحرب، فيما يلي نناقش هذه محددات التي تمثل خصائص تميز الحرب السيبرانية، باعتبارها نوع جديد من الحروب.

أ. تغير الفواعل والأهداف: أوجدت ثورة المعلومات مجالًا خامسا للحروب ليس حكرا على الجهات الفاعلة من الدول فقط، ولكن أيضًا الجهات الفاعلة من غير الدول بسبب التكاليف المنخفضة نسبيًا (Westerburger, 2014, p37)مع احتياجات، وأهداف، ونوايا مختلفة،(Sigholm, 2013, p02) فتحت الأبواب لحرب غير متكافئة، وغير نظامية. (Westerburger, 2014, p09) مؤشرات هذا التحول يعكس التغير في طبيعة الفواعل والأهداف:

تبقى الدولة هي أهم فاعل في الفضاء السيبراني تمامًا كما هو الحال في مجال الحرب التقليدية. فجميعها لديها القدرة والدافع للانخراط في الحرب، والنزاع في الفضاء السيبراني، من أجل ضمان بقائها وتحقيق مصلحتها الذاتية، فمن المنطقي أن تكون الدول على استعداد تام ومجهزة للنشاط في الفضاء السيبراني، بالنظر إلى حقيقة أن الأعداء المحتملين سيتصرفون وفقًا لذلك، وعليه المصالح الحيوية للدول في المستقبل لا يمكن تأمينها إلا إذا كانت الدولة قادرة أيضًا على النشاط في هذا المجال الجديد. (Westerburger, 2014, p09)

(سيغولم جوهان) Sigholm, Johan في مقاله "الفواعل من غير الدول في الفضاء السيبراني" أنّ يرى الأحداث الأخيرة أظهرت أن الجهات الفاعلة من غير الدول تلعب أيضًا أدوارًا رئيسية في هذه الحرب، وأحداث استونيا في ربيع 2007 مثال على مشاركتها في الحروب السيبرانية. (Sigholm, 2013, p02)، وفي حربها ضد تنظيم الدولة الإسلامية أعلنت الولايات المتحدة رسميًا في عام 2016 أن القيادة السيبرانية الأمريكية تنشط ضد "**داعش**" لقطع الاتصالات عليها، عن طريق التأثير على شبكاتها، وإجبارها على توقيف نشاطها في التجنيد، والتخطيط، ونقل الموارد. كانت هذه الأنشطة جزءا لا يتجزأ من الأنشطة العسكرية الشاملة، وعلى الرغم من أن تنظيم الدولة الإسلامية، ليس دولة فاعلة من المنظور القانوني (كما لم تعترف به الدول)، إلاّ أنها كانت مساوية للدولة من المنظور العسكري. (Saalbach, 2019, p49)

وفي تغير الأهداف: شُنت الحروب القديمة من أجل المصالح الجيوسياسية أو الأيديولوجية، أما في الحرب السيبرانية فهدفها الرئيسي، **هو الحصول على المعلومات وتوزيعها**، وكذلك التشويش على جهاز العدو

لمعرفة مجال ميدان المعركة (http://bit.ly/2BZNHxi). إذا تستهدف الحرب السيبرانية البنية التحتية المعلوماتية للقطاعات العسكرية، والحكومية والاقتصادية، كما تستهدف تغيير البيئة الثقافية والفكرية للخصوم، لتستخدمها الحكومات والأفراد كسلاح استراتيجي، وأداة هامة في الحروب الحديثة بين الدول،

ب.أدوات الحرب السيبرانية: هي رموز الحاسوب مصممة لاستخدامها، بهدف تهديد أو إلحاق ضرر جسدي، أو وظيفي، أو تقني بالهياكل، أو الأنظمة أو حتى الأشخاص،. والأسلحة،.وهذا ما ذهب إليه **(ريد)** بقوله هي "**أدوات لإلحاق الضرر**".(Brandon and Manes, 2015, P30) وتعتمد القوة السيبرانية بصفة عامة: على الأجهزة والبرامج:

الأجهزة: وهي الأدوات الميكانيكية، والمغناطيسية، والإلكترونية، والكهربائية، التي تشتمل على نظام الحاسوب، مثل وحدة المعالجة المركزية، أو محرك أقراص، أو لوحة المفاتيح أو الشاشة. كما تعتبر الكابلات والأقمار الصناعية، وأجهزة التوجيه وشرائح الحاسوب، وما شابه ذلك جزءا من هذه الأجهزة (Schreier, 2015, P103)

البرامج: وهي سلاح رئيسي في الحرب السيبرانية، تتكون من البرامج المستخدمة لتوجيه عمليات الحاسوب واستخداماته، والبرامج الضارة هي الأدوات التي تملكها الدول والتي يمكنها أن تلحق الضرر بخصومها. (Brandon and Manes, 2015, P30) حدد "توماس ريد" أربعة أساليب أساسية (أسلحة weapons) تستخدم في الحرب السيبرانية:

لغة الاستعلام الهيكلية (Structured Query Language(SQL: الحقن أو البرمجة النصية للمواقع، لتشويه صفحات الويب الخاصة بالضحايا أو إتلافها، يستحوذ هذا الشكل من الفيروسات على الموقع لبضع ساعات أو أيام ويعرض نصوصًا أو صورًا تهدد موقع الضحية أو تسيء إليه. مثلا في عام 2008، قام المتسللون الروس بتشويه العديد من المواقع الحكومية، على الرغم من أن هذه الأساليب ناعمة إلى حد ما لكن يكون لها آثار نفسية كبيرة. (Brandon and Manes, 2015, P34)

الحرمان من خدمة الموزع Distributed denial of service(DDoS): تلعب هجمات الحرمان الموزع دورًا رئيسيًا في الحرب السيبرانية، وهي محاولة لجعل مورد الحاسوب غير متوفر للمستخدمين المقصودين به، من خلال هجمات منسقة لأجهزة الحاسوب أو أجهزة أخرى.(Saalbach, 2019, p38) وهو الأسلوب الذي استخدمه المتسللون الروس في نزاع الجندي البرونزي عام 2007 ضد إستونيا، أين تم الاستيلاء على الحكومة والمواقع الخاصة الهامة من قبل شبكات الزومبي، وإغلاقها بشكل فعال لعدة أيام، التأثير الرئيسي لهذا الأسلوب هو التعطيل المؤقت للخدمة. (Brandon and Manes, 2015, P34)

الاختراقات Intrusions: المستوى الثالث من الأساليب المستخدمة في الحرب السيبرانية، وهي أكثر استهدافًا وبالتالي يمكن أن تكون أشد من التشوهات والتخريب فيما يتعلق بالضرر طويل الأجل. تعتمد على برامج فعالة لسرقة المعلومات الحساسة من المواقع الآمنية، ويمكن أن يكون لهذه الأساليب آثار مدمرة على المصالح الوطنية للدولة. (Brandon and Manes,2015, P35)

التسلل Infiltrations: هو المصطلح الذي يستخدمه لتصنيف ما يعرف باسم أكثر البرامج الضارة، يختلف عن الاختراقات حيث يتم استخدام طرق مختلفة لاختراق الشبكات المستهدفة. أهم الطرق الرئيسية للتسلل: القنابل المنطقية، الفيروسات، الديدان. (Brandon and Manes,2015, P35)

ج .الخصائص الأداة السيبرانية: تحتوي خاصية القتال السيبرانية على عدد من السمات الفريدة. على عكس الأدوات العسكرية الأخرى، على سبيل المثال: يمكن أن تكون آثارها فورية وعالمية، بالإضافة إلى ذلك، وسائل الإنترنت مُتاحة لكل من الجهات الحكومية، وغير الحكومية، وباعتبارها أداة عسكرية جديدة نسبيًا، فهي محاطة أيضًا بقدر كبير من عدم اليقين، ما يجعل إسناد السلوكات السيبرانية إلى الجهات الفاعلة أمرًا صعبًا، وهذه الصعوبة من المحتمل أن تكون في وقت الحرب أقل من وقت السلم. (Mahnken , 2011, P58) علاوة على ذلك، القيود التقنية التي تمنع ضحية الهجوم السيبراني من التعرف على المهاجم في الفضاء السيبراني، يؤدي إلى عدم القدرة على ردع المعتدي المحتمل مجهول الهوية(http://bit.ly/2BXXEv9)

ورغم أن الهجمات السيبرانية حسب عدد من المحللين قدرتها محدودة، لا تنتج أي آثارا فتاكة مباشرة، ولها قدرة محدودة على إلحاق الضرر على نطاق أوسع، حتى في حالة وقوع هجمات على البنية التحتية الاقتصادية للدولة، إلا أن **الردع السيبراني المعقد**، الذي يعني أنّه في حالة فشل الهجوم السيبراني لقوة أضعف في تحقيق أهدافها، يجعلها تواجه انتقاما مدمرا، من قبل قوة الأقوى التي ستمتلك خيارات أكثر فتكًا للرد، ما يسمى في مصطلحات الردع النووي، **هيمنة التصعيد**. علاوة على ذلك، لا يتوجب حصر تلك الاستجابة في المجال السيبراني، يمكن أن يشمل الرد في مجالات أخرى (Mahnken, 2011, P59-60) وتوظيف مجموعة كاملة من القدرات العسكرية كرد فعل.

إضافة الى ما سبق تتحول القدرات السيبرانية إلى مكمّلة غير مكلفة للقدرات العسكرية للدولة، على سبيل المثال أجرت كل من الولايات المتحدة وإسرائيل هجومًا سيبرانيًا Stuxnet ضد البنية التحتية النووية الإيرانية، تحقيق هذه النتيجة سيكون أكثر تكلفة وصعوبة بالوسائل العسكرية التقليدية. (Westerburger, 2014, p09)

تفرض خصائص الأداة السيبرانية أرضية نظرية جديدة فيما يتعلق بدور "المعلومات" في بيئات الحرب، وأنّها ليست مجرد مجموعة جديدة من التقنيات العملياتية، وإنما هي منهج جديد للحرب يستدعي مقاربات جديدة للخطط والاستراتيجيات، وأشكال جديدة من العقيدة والتنظيم.

3.الحرب السيبرانية وتطور الاستراتيجية العسكرية للدول

يناقش هذا المحور تأثير الأسلحة السيبرانية أو ما يصطلح عليه بالأسلحة الافتراضية أو المرنة، على المذهب العسكري، والاستراتيجية الدفاعية للدول.

أ.نقل البيئة القتالية إلى الفضاء السيبراني والتحول في المذهب العسكري: أدى الفضاء السيبراني إلى انتقال الحروب من صناعية قائمة على المواجهة، إلى تجنب الصراع الاستنزافي، ودفع كل دولة تعتمد على البنية التحتية لتكنولوجيا المعلومات، إلى انتهاج عقيدة عسكرية جديدة، من خلال تطوير استراتيجيات وقدرات لحماية، وممارسة القوة الوطنية، وتكييف بعض التكتيكات، والمنتجات التقليدية التي يحتاجها الجيش، مع

بيئة الفضاء السيبراني. وتدريب المنظمات على تطوير خطط، وعقيدة جديدة. (Andress, Winterfeld, 2011, P xxiv,) أهم التحولات في المذهب العسكري في العصر الرقمي هي:

كسب الحروب من خلال ضرب القلب الاستراتيجي للهياكل السيبرانية للخصم: نظم المعرفة، والمعلومات والاتصالات، فمذهب الحرب السيبرانية يسمح بتطوير القدرة على استخدام القوة، ليس فقط بطرق تقلل من التكاليف التي يتحملها الطرف الذي يشن الهجوم، ولكنها تتيح أيضًا تحقيق النصر بدون الحاجة إلى تعظيم تدمير العدو. (http://bit.ly/2BXXEv9).

تعتبر الحرب السيبرانية من وجهة نظر عسكرية، نوعا موازيا لحرب المعلومات الاستراتيجية، **وتساعد أدوات الحرب السيبرانية في التخلص من "ضباب الحرب" 'fog of war' (لكلاوزوفيتش)**، أي إزالة عدم القدرة على التنبؤ في ساحة المعركة. (F. G. Hoffman, 2017)، أضف إلى ذلك كونها من مخرجات الثورة الرقمية والمعلوماتية في الشؤون العسكرية، أدت إلى انتقال نوعية القتال من مفهمة **(كلاوزفيتزش)** المرتكزة على المعركة، إلى مفهمة **(صان تزو)** المرتكزة على قاعدة المعرفة في القتال. (Kane, Lonsdale, 2012, p72).

كما أنتج الفضاء السيبراني نمطا آخر من الحرب: حرب المعلومات (حرب المعلومات الاستراتيجية)، والتي يتم تعريفها على أنها "هجوم سيبراني على هياكل تكنولوجيا المعلومات الحيوية للخصم المدني والعسكري، يمكن أن يكون هذا النوع من الحرب موازيًا للحرب السيبرانية، وبهذا المعنى: يمثل ما يعادل القصف الاستراتيجي في العصر الصناعي. (http://bit.ly/2BZNHxi)

ب.إستراتيجية الدفاع السيبراني: إلى حد الأن لا زال فيه عدم الاتفاق حول الاستراتيجية الدفاعية الفعالة التي يجب تنفيذها لمواجهة هذه الحرب، ونظرا لكونها نوعا من الحروب الخاطفة، سيتطلب معرفة متقدمة بالبرامج الضارة التي يتم تطويرها في أنظمة يحتمل أن تكون معادية، إضافة إلى الاستجابة التلقائية، وإجراء رد فعل وقائي لنزع سلاح الهجوم، ولكي يكون الدفاع النشط فعالاً، يجب تفويض السلطة بموجب قواعد الاشتباك المدروسة المتقدمة مسبقًا. (http://bit.ly/2q8Ptcy).

في الولايات المتحدة الأمريكية تم إصدار استراتيجية وزارة الدفاع للعمل في الفضاء السيبراني في جولية 2011، وتضم خمس مبادرات:(Andress, And Others, 2014, P55)

• المبادرة الاستراتيجية الأولى: تعامل الفضاء السيبراني كمجال عملياتي لتنظيم، وتدريب، وتجهيز المعدات بحيث تتمكن وزارة الدفاع من الاستفادة الكاملة من إمكانات الفضاء السيبراني.

• المبادرة الاستراتيجية الثانية: توظيف مفاهيم جديدة للتشغيل الدفاعي لحماية شبكات وأنظمة وزارة الدفاع.

• المبادرة الاستراتيجية الثالثة: شراكة مع الإدارات والوكالات الحكومية الأمريكية الأخرى، والقطاع الخاص لتمكين استراتيجية الأمن السيبراني للحكومة بأكملها.

• المبادرة الاستراتيجية الرابعة: بناء علاقات قوية مع حلفاء الولايات المتحدة والشركاء الدوليين لتعزيز الأمن السيبراني الجماعي.

• المبادرة الاستراتيجية الخامسة: الاستفادة من براعة الأمة من خلال قوة عاملة سيبرانية استثنائية وابتكار تكنولوجي سريع.

عموما يشمل الدفاع السيبراني على ثلاث فئات متكاملة:

الدفاع السيبراني الاستباقي: وهي الأنشطة التي تحمي البيئة السيبرانية، وتحافظ على أعلى كفاءة للبنية التحتية السيبرانية، والوظائف المهمة .(Galinec, and others, 2017, p277)، من خلال الابتكار لتعزيز الفعل السريع أسرع من المنافسين الاستراتيجيين، وحماية الشبكات والأنظمة والوظائف والبيانات (Http://Bit.Ly/2rkpkow)، ومواكبة التهديدات، والتكنولوجيات سريعة التطور في الفضاء السيبراني، الحفاظ على السلام والأمن السيبراني من خلال تعزيز قدرة الدول، بالتنسيق مع الحلفاء والشركاء - على ردع ومعاقبة أولئك الذين يستخدمون أدوات السيبرانية لأغراض ضارة. (Http://Bit.Ly/2rkpkow)

الدفاع السيبراني النشط: يوقف أو يحد من أضرار النشاط السيبراني للخصم، (Galinec, and others, 2017, p277) ، وردع الأنشطة السيبرانية الضارة: باستخدام جميع أدوات القوة الوطنية لردع الأعداء عن القيام بأي نشاط ضار في الفضاء السيبراني، الذي يهدد المصالح الوطنية، وإعطاء الإدارة الأولوية لتأمين معلومات وزارة الدفاع . يجب على الدولة حماية شبكاتها من خلال هيئاتها التشريعية، تأكد من سد أي ثغرات قائمة في قانون الإنترنت. (Http://Bit.Ly/2rkpkow)

فهم طبيعة التهديدات فلا يمكن للمرء أن يقاوم بشكل فعال شيئًا لا يفهمه، تثقيف القوى العاملة (الموظفين والمقاولين) -الأمن هو شيء يعتبره معظمنا أمرا مفروغا منه، حتى يحدث شيء سيء لنا أو لأحد أصدقائنا. هذا يجب أن يتغير. في هذا السياق، يعد التعاون الدولي ذا أهمية كبيرة. في المستوى الرابع، إن لم يكن قبل ذلك، تُستكمل هذه الجوانب بحماية البنية التحتية الحيوية (Cavelty, 2010, P03).

الدفاع السيبراني التفاعلي: يعمل على استعادة الفعالية، أو الكفاءة بعد الهجوم السيبراني الناجح، هذه الفئات تشكل سلسلة متصلة من أنشطة الأمن السيبراني التي تحدث بشكل مستمر وفي وقت واحد على الشبكات.(Galinec, and others, 2017, p277)، ووضع سياسات لأمن المعلومات - ومراجعتها (بشكل دوري).

هيمنة التصعيد Escalation Dominance، من خلال القدرة على الجمع بين الوسائل السيبرانية، والأدوات العسكرية الأخرى للقيام بحملة أسلحة مشتركة(Mahnken, 2011, P59-60).

خاتمة:

تشكل الحرب السيبرانية نمطا جديدا من الحروب في العصر الرقمي، رغم المشككين من المفكرين الاستراتيجيين الذين يعتمدون على منطق (كلاوزفيتش) ليجادلوا بأن الخطر السيبراني مبالغ فيه لأن التكنولوجيا الرقمية هي مجرد تطور في السياقات العامة للحرب لكن لا تغير في طبيعة الحرب، ويستدلون بأن الهجمات السيبرانية ليست **عنيفة**، وبالتالي لا ترقى إلى أن تكون فعلا حربيا.

تستمد الحرب السيبرانية جوهرها من تعريف كلا من المنظرين (**كلاوزوفيتش**)، و(**صان تزو**) بما أنّ الهدف النهائي للحرب هو إجبار العدو على الامتثال لإرادة الفرد، وأن أفضل شكل للحرب هو الشكل الذي يُهزم فيه العدو دون قتال، نجد أنه من خصائص الأداة السيبرانية القدرة في تحقيق الأهداف السياسية دون

الحاجة إلى اللجوء إلى الاشتباكات العنيفة، لكن تأثيرها لا يختلف عن تأثير الأسلحة التقليدية، ما يجعلنا نقول أنّ الحرب المستقبلية لا تحتاج بالضرورة إلى الاحتكاك، والعنف في إدارتها، وإنما يحتاج مفهوم العنف باعتباره أهم سمة تعكس طبيعة الحرب الثابتة حسب الطرح (**الكلاوزفيتشي**)إلى توسيع تكيفا مع متغيرات العصر الرقمي.

يتضمن هذا النوع الجديد من الحروب على عوامل جذب أهمها القدرة والدقة في تحقيق الأهداف جعلتها أوسع وأسرع انتشارا، كما أنها تتميز بالديناميكية، والقدرة على الانتشار من حرب في المجال السيبراني إلى حرب عسكرية في الواقع، كما أنها تمنح للجهات الفاعلة العسكرية الأضعف مزايا غير متماثلة، سهلت الهجوم، بينما الدفاع يزداد صعوبة، وإخفاء هوية المهاجم يقوض **الردع**.

التحديات التي طرحتها الحرب السيبرانية، أوجبت ضرورة المراجعة الاستراتيجية للقدرات الدفاعية عن مراكز ثقل الدولة التي أصبحت أكثر عرضة للاختراق، والتهديد مع صعوبة تحديد الجهة الفاعلة، وكذلك المراجعة الاستراتيجية للقدرات الهجومية.

قائمة المراجع

1. Adress Jason, Winterfeld Steve, (2011) , Cyber Warfare Techniques: Tactics And Tools For Security Practitioners; LONDON; Syngress Is An Imprint Of Elsevier.
2. Braillard Philippe, Gianluca Maspoli, La Révolution Dans Les Af2faires Militaires : Paradigmes Stratégiques, Limites Et Illusions, On The Site : http://bit.ly/2BZNHxi (06/07/2019)
3. Brandon Valeriano and Manes Ryan., (2015), Cyber War versus Cyber Realities: Cyber Conflict in the International System, New York, Oxford.
4. .Cavelty Dunn Myriam, (April 2010), Cyberwar: Concept: Status Quo, And Limitations Political, Center For Security Studies, Analysis In Security Policy, No. 71.Pp01-04.
5. Colin Gray, (2006), Strategy and History, London and New York, routledge: Taylor & Françoi group.
6. Colin S. Gray, War, (2007), Peace and International Relations: An Introduction to Strategic History, London & New York, Routledge: Taylor & Francis Group.
7. Department Of Defense Cyber Strategy, 2018, In Site: (Http://Bit.Ly/2rkpkow)
8. Dragan Z. Damjanović , (2017), Types Of Information Warfare And Examples Of Malicious Programs Of Information Warfare, Vojnotehni Čki Glasnik / Military Technical Courier, Vol. 65, Issue 4, Pp1045-1059.
9. Ducheine Paul, Cyber warfare is taking place!, Internationale Spectator, in site: http://bit.ly/2N3rq84 (08/07/2019)
10. .F. G. Hoffman, (winter2017-18), Will War's Nature Change in the Seventh Military Revolution? , US Army War College: Parameters, VOL. 47 NO. 4, Pp19-31.

11. Galinec Darko, and others, (2017), Cybersecurity and cyber defence: national levelstrategic approach, Automatika, VOL. 58, NO. 3, Pp, 273-286
12. Jason Andress, And Others, (2014), Cyber Warfare: Techniques, Tactics And Tools For Security Practitioners, Usa, Elsevier.
13. 13.Johan Sigholm, (2013), Non-State Actors In Cyberspace Operations, Journal Of Military Studies, Vol. 4, No 1, Pp01-3.
14. John Arquilla and David Ronfeldt, Cyberwar Is Coming!, in the site: http://bit.ly/2BXXEv9
15. Joint Chiefs of Staff, Joint Publication 1-02, Washington D.C., US Department of Defense, 12 April 2001, in the site : http://bit.ly/33d3Ryu
16. Kaldor Marry, (2012), New And Old War, USA, Cambridge.
17. Kane Thomas, Lonsdale David J, (2012), Understanding Contemporary Strategy, London and New York, routledge: Taylor & Françoi group.
18. Kennethv.Peifer,B.S., (December 1997)"Ananalysisofunclassifiedcurrent And Pending Air Force Information Warfare And Information Operations Doctrine And Policy",Graduate School Of Logistics And Acquisition Management Air Force Institute Of Technology.
19. Levieux François, (Novembre 2005), La défense et les technologies de l'information et de la communication, ANNALES DES MINES, ISSN 1148-7941, Pp68-72.
20. Lonsdale David J, The Nature of War in the Information Age: Clausewitzian Future, (2004), London , New York,Frank Cass: Taylor & Francis Group.
21. Mahnken Thomas, (june2011), bloodless yet potentially devastating new method of warfare, America's Cyber Future Security and Prosperity in the Information Age , volume 11. Pp57-63.
22. Mbuthia Rex, Cyber Warfare versus Information Warfare: Two Very Different Concepts, in the site: http://bit.ly/2OH4UkG
23. Nye Joseph, Nuclear Lessons for Cyber Security, in the site: http://bit.ly/2q8Ptcy
24. Renouf Jean, The Rise of Cyber and the Changing Nature of War, in the site: http://bit.ly/33qNGNR
25. Rid Thomas, (2013), Cyber War Will Not Take Place, New York, Oxford University Press.
26. Saalbach Klaus-Peter, Cyber war Methods and Practice, (july2019), Germany, Arbeitspapier.
27. Schreier Fred, (2015), On Cyberwarfare, Dcaf Horizon Working Paper No.7.
28. Westerburger Steffen, (2014), Cyber Conflict in the 21st Century: The Future of War and Security in a Digitalizing World, Master Thesis International Relations, Radboud University.